

Data Mining and Counter-Terrorism: The Use of Telephone Records as an Investigatory Tool in the “War on Terror”

BRYAN D. KREYKES*

Abstract: In December 2005, media outlets reported the existence of a secret government program aimed at tracking terrorist activity through the use of telephone records. As part of that program, the National Security Agency (“NSA”) and Federal Bureau of Investigation (“FBI”) reportedly demanded that telephone companies turn over confidential customer records to government agencies. The program, commonly referred to as “data mining,” involves scrutinizing trillions of call records, searching for suspicious patterns of communication between domestic phone numbers and those of suspected foreign terrorists. Once a link between a suspected foreign terrorist and a domestic telephone number is found, records of calls originating from that number are examined. The records of recipients of those calls are then examined for signs of communication with suspected terrorists. Due to the extreme secrecy of the program, both its legality and its statutory basis remain unclear.

This article examines the various statutory schemes under which the NSA and FBI data mining program may have been conducted. It begins by summarizing the process of data mining and analyzing its usefulness as a counter-terrorism tool. It then discusses the general statutory prohibition on telephone companies revealing customer records and the statutory exceptions to that ban. The article then addresses the incentives faced by phone companies under the current statutory scheme and the resulting impact on consumer privacy expectations. Under federal law, telephone companies that reveal customer records pursuant to national security requests by the

* The author would like to thank the following: Professors Steven Holmes and David Golove of the NYU Law & Security Colloquium for their insight and direction, the faculty and staff of NYU School of Law for their help with research materials, and, as always, Doug and Jeannie Kreykes for their constant support.

NSA, FBI, and other agencies are insulated from the liability based on those revelations. That insulation from liability, coupled with the threat of adverse government action, creates an overwhelming incentive for telephone companies to disclose records when served with a request. This article concludes by arguing that data mining leads to a large number of false positive identifications of potential terrorists which, in turn, must be discredited using more traditional law enforcement techniques. Due to the time and manpower required to track down those false positive identifications, this article concludes that data mining is an inefficient use of the government's limited resources, and recommends traditional law enforcement techniques as a more effective means of pursuing the domestic portion of the "War on Terror."

I. INTRODUCTION: DATA MINING AND TELEPHONE RECORDS

In December 2005, media outlets exposed the existence of a secret government program aimed at tracking and preventing terrorist activity.¹ According to reports, the program involved demands by the National Security Agency ("NSA") and Federal Bureau of Investigation ("FBI") that telephone companies disclose customer records.² The records demanded included details of who has called or been called by a particular telephone user, how long the calls lasted, what time of day they were made, and the number of times calls were made to or received from any other phone number.³

The type of counter-terrorism program for which the records were reportedly requested is known as "data mining."⁴ Data mining involves scrutinizing trillions of call records in a search for patterns of communication between domestic phone numbers and those of suspected foreign terrorists.⁵ Once a link between a suspected foreign terrorist and a domestic telephone number is found, records of calls originating from the domestic number are examined.⁶ Recipients of those calls are then examined for signs of communication with suspected terrorists.⁷ Factors such as time, duration, origin, destination, frequency, and quantity of calls are weighed in an attempt

¹ See, e.g., Eric Lichtblau and James Risen, *Domestic Surveillance: The Program; Spy Agency Mined Vast Data Trove*, *Officials Report*, N.Y. TIMES, Dec. 24, 2005, at A1.

² See, e.g., Lichtblau and Risen, *supra* note 1, at A1; Lowell Bergman et al., *Domestic Surveillance: The Program; Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, at A1; *Congress Demands NSA Spying Answers*, CBS NEWS, May 11, 2006, <http://www.cbsnews.com/stories/2006/05/11/politics/main1609261.shtml>.

³ Lichtblau and Risen, *supra* note 1, at A1.

⁴ Bergman et al., *supra* note 2, at A1; see also American Civil Liberties Union, *Eavesdropping 101: What Can the NSA Do?* Jan. 31, 2006, <http://www.aclu.org/safefree/nsaspying/23989res20060131.html>.

⁵ Bergman et al., *supra* note 2, at A1.

⁶ See, e.g., Lichtblau and Risen, *supra* note 1, at A1; American Civil Liberties Union, *supra* note 4.

⁷ See, e.g., Lichtblau and Risen, *supra* note 1, at A1; American Civil Liberties Union, *supra* note 4.

to discover suspicious patterns of communication.⁸ If analysis of the calls shows a pattern of communication between suspected terrorists and a particular phone number, the NSA instructs the FBI to investigate the individual to whom that number belongs.⁹

Data mining is unique because it does not involve the real-time tracing of calls traditionally utilized by law enforcement in so-called “pen register” or “trap and trace” programs. Under a pen register program, a device is used to monitor a particular phone number and decode outgoing electronic signals, thereby revealing which numbers are dialed from that phone.¹⁰ Under a trap and trace program, a device that decodes the electronic signals accompanying incoming calls is used to monitor a particular phone number.¹¹ Federal law requires government entities to obtain a court order before using pen registers or trap and trace devices to monitor the incoming or outgoing calls from a suspect’s telephone.¹² Government agents may

⁸ See, e.g., Lichtblau and Risen, *supra* note 1, at A1; American Civil Liberties Union, *supra* note 4.

⁹ See, e.g., Lichtblau and Risen, *supra* note 1, at A1; American Civil Liberties Union, *supra* note 4.

¹⁰ See 18 U.S.C. § 3127(3). Under that section, the term “pen register” is defined as

[A] device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

¹¹ See 18 U.S.C. § 3127(4) (2001). Under that section, the term “trap and trace device” is defined as

[A] device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

¹² 18 U.S.C. § 3121(a) (2001).

obtain a court order under 18 U.S.C. § 3123 to monitor phone traffic between numbers within the geographic United States, pursuant to a finding by the court that an “attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.”¹³ In order to use a pen register or trap and trace device to monitor incoming or outgoing phone traffic between a phone number in the United States and numbers in foreign countries, government agents must obtain a court order from either a magistrate judge or the special court established by the Foreign Intelligence Surveillance Act of 1978 (“FISA”).¹⁴ In contrast to the use of pen registers or trap and trace devices, which require a court order and the installation of special equipment, data mining involves obtaining and examining the records of millions of individuals without installing any special monitoring equipment or obtaining a court order.¹⁵

Data mining programs also differ from “wiretapping.” Under wiretap programs, the spoken contents of telephone conversations are monitored or recorded.¹⁶ “Contents” are defined under federal law as “any information concerning the substance, purport, or meaning of [a] communication.”¹⁷ The recent NSA and FBI disclosure requests reportedly did not involve the monitoring of spoken content.¹⁸ Rather, the requests were limited to records of electronically-transmitted data about the origin, destination, duration, frequency, and quantity of calls.¹⁹

¹³ 18 U.S.C. § 3123(a)(1) (2001).

¹⁴ See 50 U.S.C. §§ 1805, 1861 (2006).

¹⁵ See, e.g., Lichtblau and Risen, *supra* note 1, at A1; American Civil Liberties Union, *supra* note 4.

¹⁶ See *Smith v. Maryland*, 442 U.S. 735, 741–42 (1979) (drawing the distinction between intrusions which monitor the contents of communications and those that monitor only the telephone numbers dialed or numbers from which a call was received).

¹⁷ 18 U.S.C. § 2510(8) (2002).

¹⁸ See CBS NEWS, *supra* note 2 (“The program does not involve listening to or taping the calls. Instead it documents who talks to whom in personal and business calls . . . by tracking which numbers are called.”); Lichtblau and Risen, *supra* note 1, at A1 (“The N.S.A. has sought to analyze communications patterns to glean clues from details like who is calling whom, how long a phone call lasts and what time of day it is made, and the origins and destinations of phone calls.”).

¹⁹ See CBS NEWS, *supra* note 2; Lichtblau and Risen, *supra* note 1, at A1.

The government's data mining program is an undesirable development and should be discontinued. The program creates two principal problems. First, it uses a little-known statutory scheme to create perverse incentives for telephone companies to compromise the privacy of their customers. Second, the program ineffectively utilizes limited government resources by creating millions of false positive suspects who must then be investigated and eliminated by traditional law enforcement methods.

II. CONFIDENTIALITY OF TELEPHONE RECORDS

When served with NSA or FBI requests for records, phone companies face the dilemma of whether to risk customer lawsuits by disclosing the records, or to risk punitive action by refusing to comply with the government's request. Federal law governing telephone records attempts to balance the confidentiality interests of telephone customers against the government's duty to assure national security. In order to maintain that balance, the law prohibits telecommunications providers from disclosing customer records except in narrowly defined circumstances. The general prohibition on disclosure is contained in 18 U.S.C. § 2702 and 47 U.S.C. § 222. Exceptions to that prohibition are contained in 18 U.S.C. § 2703 and 18 U.S.C. § 2709.²⁰

A. THE GENERAL PROHIBITION ON DISCLOSURE OF CUSTOMER RECORDS: 18 U.S.C. § 2702

The general prohibition on disclosure of customer records is contained in 18 U.S.C. § 2702. It provides that "[e]xcept as provided in subsection (b) or (c), a provider of . . . an electronic communication service to the public shall not knowingly divulge a record or other

²⁰ The Foreign Intelligence Surveillance Act also allows limited access to telephone records for the purposes of counter-terrorism investigations. See 50 U.S.C. § 1861(a)(1). This article does not discuss FISA provisions governing disclosure of customer records by telephone companies because a court order is required to compel disclosure under the FISA. See 50 U.S.C. § 1861(b)(1) (requiring application to a magistrate judge or the special court established by the FISA in order to obtain a court order demanding disclosure of customer records). The recent requests for telephone records by the NSA and FBI reportedly did not involve a court order. See, e.g., Lichtblau and Risen, *supra* note 1, at A1; Bergman et al., *supra* note 2, at A1; CBS NEWS, *supra* note 2; American Civil Liberties Union, *supra* note 4.

information pertaining to a subscriber to or customer of such service . . . to any government entity.”²¹ “Electronic communication” is defined by 18 U.S.C. § 2510 as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system.”²² That definition encompasses electronic impulses containing dialing, routing, addressing, or signaling information transmitted or received when an outgoing call is made or an incoming call is answered that are recorded by phone companies for the purposes of billing or recordkeeping.²³ “Wire” and “oral” communications, which include the spoken and auditory content of telephone conversations, are specifically exempted from the definition of “electronic communication.”²⁴ The definition of “electronic communication,” therefore, arguably includes telephone records showing that a call was made or received and billing records pertaining to the duration, quantity, and frequency of such calls, but does not include voice information exchanged by the parties to the call.²⁵

The exceptions to the general prohibition on disclosure of customer records contained in subsection (b) of 18 U.S.C. § 2702 pertain only to information about the content of communications.²⁶ As such, those exceptions do not apply to the recent NSA and FBI

²¹ 18 U.S.C. § 2702(a)(3) (2006).

²² 18 U.S.C. § 2510(12) (2002).

²³ See 18 U.S.C. § 3127(4) (referring to “incoming electronic impulses” that “identify the originating number or other dialing, routing, addressing, and signaling information” captured by so-called “trap and trace” devices); 18 U.S.C. § 3127(3) (referring to the “dialing, routing, addressing, or signaling information transmitted” by outgoing calls and stating that “such information shall not include the contents of any communication, but such term does include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as incident to billing”). See also *Smith*, 442 U.S. at 741 n.1 (describing a “pen register” as a device that “records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the phone is released” and distinguishing the record of a call being made that is generated by such electrical impulses from records of the spoken content of such a call).

²⁴ 18 U.S.C. § 2510(12)(A) (2002).

²⁵ See *Smith*, 442 U.S. at 741 (discussing records generated by decoding electronic impulses accompanying a phone call that are recorded by a pen register and distinguishing those records from the spoken content of the call).

²⁶ See 18 U.S.C. § 2702(b) (2006).

disclosure requests, which were limited to records of electronically-transmitted data about the origin, destination, duration, frequency, and quantity of calls.²⁷ The exceptions to the general prohibition on disclosure contained in subsection (c) of 18 U.S.C. § 2702 allow telecommunications providers to divulge customer records “as otherwise authorized in section 2703.”²⁸ That statute, and the circumstances in which it authorizes the release of customer records, is discussed in Section III.A, below.

**B. THE PROHIBITION ON DISCLOSURE OF CUSTOMER
PROPRIETARY NETWORK INFORMATION:
47 U.S.C. § 222**

Records regarding the “type, destination, location, and amount of use of a telecommunications service” that are obtained by a phone company “solely by virtue of the carrier-customer relationship” are defined under federal law as “customer proprietary network information” (“CPNI”).²⁹ Under 47 U.S.C. § 222, CPNI may only be disclosed “as required by law or with the approval of the customer.”³⁰ Therefore, the prohibition on disclosure of CPNI can be circumvented by any other federal statute’s authorization to divulge that information.

III. STATUTES REQUIRING DISCLOSURE OF CUSTOMER RECORDS

Two principle statutes, 18 U.S.C. §§ 2703 and 2709, require telephone companies to turn customer records over to a government entity when that entity serves the company with a specific type of demand. Those laws present themselves in the form of narrow exceptions to the general prohibition on disclosure of customer records. Telephone companies are immune from liability for disclosures made pursuant to those exceptions.

²⁷ See CBS NEWS, *supra* note 2; Lichtblau and Risen, *supra* note 1, at A1.

²⁸ 18 U.S.C. § 2702(c)(1) (2006).

²⁹ 47 U.S.C. § 222(h) (1999).

³⁰ 47 U.S.C. § 222(c)(1) (1999).

A. THE WARRANT, COURT ORDER, AND ADMINISTRATIVE
SUBPOENA EXCEPTIONS:
18 U.S.C. § 2703(c)

Telephone companies are required by 18 U.S.C. § 2703(c) to turn over customer records to a government entity without customer consent when (1) served with a warrant demanding disclosure, (2) served with a court order demanding disclosure, (3) the government entity submits a formal written request for records relating to telemarketing fraud, or (4) pursuant to an administrative subpoena.³¹ The law requires phone companies to disclose information pertaining to the customer's name, address, local and long distance connection records (including call duration and frequency), the length of subscription and type of service subscribed to, telephone number or other information used to identify the subscriber, and payment records (including credit card or bank account numbers).³²

No law requires that the telephone customer whose records are divulged to the government pursuant to a warrant, court order, written request for records relating to telemarketer fraud, or administrative subpoena, be informed that his or her records have been disclosed. The government entity to whom the records are revealed is under no obligation to provide notice of the disclosure.³³ Telephone companies may be prohibited by the terms of an administrative subpoena or court order from informing customers of government demands for records, but 18 U.S.C. § 2703 itself contains no clause prohibiting companies from informing customers of a government request for records.³⁴

Even if the initial request for disclosure is made without a warrant, court order, or administrative subpoena, telephone companies are required to retain requested records for ninety days while the government entity making the request applies for an order or warrant, or goes through the process of issuing an administrative subpoena.³⁵

³¹ 18 U.S.C. § 2703(c)(1) (2006) (requiring disclosure when the company is served with a warrant, court order, or formal request relating to telemarketing fraud), (c)(2) (requiring disclosure "when the governmental entity uses an administrative subpoena authorized by a Federal or State statute").

³² §2703(c)(2).

³³ § 2703(c)(3).

³⁴ *See generally* § 2703.

³⁵ 18 U.S.C. § 2703(f)(1) (2006).

The ninety-day retention period is renewable on request by the government entity.³⁶ There is no limit on the number of times the government may request renewal.³⁷ The retention period does not take effect, however, until a request for records is made.³⁸ Nothing in 18 U.S.C. § 2703 prohibits telephone companies from disposing of records before a disclosure request is made.³⁹ Furthermore, 18 U.S.C. § 2703 does not require telephone companies to record any information in addition to the records that they normally keep.⁴⁰ Telephone companies only maintain records of metered calls for billing purposes. Records of non-metered calls are not kept, and telephone companies are not required to create records of those calls simply to comply with government disclosure requests.

Telephone companies that disclose customer records in compliance with the requirements of 18 U.S.C. § 2703 are granted immunity from both criminal and civil liability arising out of the disclosure.⁴¹ Therefore, companies cannot be held accountable by their customers or other individuals whose records are disclosed to the government pursuant to a warrant, court order, written request for records relating to telemarketer fraud, or administrative subpoena.⁴²

1. THE WARRANT EXCEPTION

Telephone companies are required to turn customer records over to a government entity when served with a warrant demanding disclosure.⁴³ In order for a government entity to obtain such a warrant, it must establish “probable cause” by articulating “facts or circumstances” sufficient to “warrant a man of reasonable caution in

³⁶ § 2703(f)(2).

³⁷ *Id.*

³⁸ See § 2703(f)(1) (stating that “upon the request of a governmental entity,” telephone companies “shall take all necessary steps to preserve records”).

³⁹ See generally § 2703.

⁴⁰ *Id.*

⁴¹ 18 U.S.C. § 2703(e) (2006).

⁴² *Id.*

⁴³ § 2703(c)(1)(A).

the belief” that a crime had been or was about to be committed.⁴⁴ The applicability of the warrant is limited to particular telephone records that are demonstrated, with some degree of certainty, to be related to the specific crime for which probable cause was shown.⁴⁵

The recent NSA and FBI requests for telephone records reportedly included records of millions of customers who were not suspected of criminal activity.⁴⁶ Those requests were reportedly made without a warrant demanding telephone companies disclose the records.⁴⁷ It is unlikely, therefore, that the requests were made pursuant to the warrant exception provided in 18 U.S.C. § 2703(c)(1)(A).

2. THE COURT ORDER EXCEPTION

When served with a court order demanding disclosure, telephone companies are required to disclose customer records to the government entity making the request.⁴⁸ In order to obtain a court order, the government entity must articulate specific facts showing that the records sought are relevant to an ongoing criminal investigation.⁴⁹ Telephone companies have the option to file a motion to quash or modify a court order requiring “unusually voluminous” disclosures.⁵⁰

⁴⁴ See *Carroll v. United States*, 267 U.S. 132, 162 (1925).

⁴⁵ *Id.*; see also U.S. CONST. amend. IV (stating that “no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized”).

⁴⁶ See, e.g., Lichtblau and Risen, *supra* note 1, at A1; Bergman et al., *supra* note 2, at A1; CBS NEWS, *supra* note 2; American Civil Liberties Union, *supra* note 4.

⁴⁷ See, e.g., Lichtblau and Risen, *supra* note 1, at A1; Bergman et al., *supra* note 2, at A1; CBS NEWS, *supra* note 2; American Civil Liberties Union, *supra* note 4.

⁴⁸ 18 U.S.C. § 2703(c)(1)(B).

⁴⁹ See 18 U.S.C. § 2703(d) (2006) (“[A] court order for disclosure under subsection . . . (c) may be issued only by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe . . . the records and other information sought are relevant and material to an ongoing criminal investigation.”).

⁵⁰ *Id.* (“[A] court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.”).

NSA and FBI counter-terrorism programs constitute ongoing criminal investigations insofar as federal law criminalizes harboring, providing support for, receiving training from, or conspiring with suspected terrorists.⁵¹ The recent NSA and FBI requests for phone records, however, were reportedly made without a court order demanding telephone companies disclose the records.⁵² It is thus unlikely that the requests were made pursuant to the court order exception of 18 U.S.C. § 2703(c)(1)(B).

3. THE ADMINISTRATIVE SUBPOENA EXCEPTION

Telephone companies are required by law to disclose customer records to the government when served with an administrative subpoena authorized by state or federal law.⁵³ The United States Supreme Court has long held that agencies have the power to issue subpoenas to gain information as long as that information is not “incompetent or irrelevant to [the agency] in the discharge of [its duties].”⁵⁴ Investigatory subpoenas will be enforced when the investigation at issue is congressionally authorized and is undertaken for a purpose that Congress has the power to command.⁵⁵ The Court has explicitly held that probable cause need not be shown for an administrative subpoena to issue.⁵⁶ All that needs to be demonstrated for an agency to overcome a challenge to its subpoena is that the agency is acting within the scope of its delegated power by carrying on an investigation, and that the information sought is relevant to that investigation.⁵⁷

⁵¹ See generally, 18 U.S.C. § 2339 (2002); 18 U.S.C. §§ 2339(A), 2339(B), 2339(C), 2339(D) (2006).

⁵² See, e.g., Lichtblau and Risen, *supra* note 1, at A1; Bergman et al., *supra* note 2, at A1; CBS NEWS, *supra* note 2; American Civil Liberties Union, *supra* note 4.

⁵³ 18 U.S.C. § 2703(c)(2) (2006).

⁵⁴ *Endicott Johnson Corp. v. Perkins*, 317 U.S. 501, 509 (1943).

⁵⁵ *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946).

⁵⁶ *Id.* (holding that “the requirement of ‘probable cause, supported by oath or affirmation,’ literally applicable in the case of a warrant, is satisfied in that of an order for production, by the court’s determination that the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry.”).

⁵⁷ *Id.*

The NSA and FBI are charged with investigating and preventing international and domestic terrorism, and therefore have the power to issue administrative subpoenas while investigating possible terrorist plots.⁵⁸ Media coverage of the recent requests for telephone records made by those agencies, however, does not reveal whether the requests were made pursuant to administrative subpoenas.⁵⁹ Given that the recent requests for telephone records were not made pursuant to a court order or warrant,⁶⁰ it is likely that they were made pursuant to either the administrative subpoena exception provided by 18 U.S.C. § 2703(c)(2), or the exception for FBI requests for records relevant to ongoing investigations of terrorist activities provided by 18 U.S.C. § 2709. The latter is discussed below.

B. FBI ACCESS TO TELEPHONE RECORDS RELEVANT TO
INVESTIGATIONS OF TERRORIST ACTIVITIES:
18 U.S.C. § 2709

In addition to the requirement that telephone companies disclose customer records pursuant to a warrant, court order, or administrative subpoena, 18 U.S.C. § 2709 requires companies to turn over subscriber information and billing records when those records are demanded pursuant to a certification issued by the FBI that the records are relevant to an ongoing counterterrorism investigation.⁶¹ Under this provision, a certification may be made by the Director of the FBI or any designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office.⁶² Since the FBI has 56 field offices, a total of 58 individuals could conceivably issue a certification under this

⁵⁸ See National Security Agency, *Introduction to NSA/CSS*, <http://www.nsa.gov/about/index.cfm> (last visited Apr. 16, 2008); Federal Bureau of Investigation, *National Security Branch*, <http://www.fbi.gov/hq/nsb/nsb.htm> (last visited Apr. 16, 2008).

⁵⁹ See, e.g., Lichtblau and Risen, *supra* note 1, at A1; Bergman et al., *supra* note 2, at A1; CBS NEWS, *supra* note 2; American Civil Liberties Union, *supra* note 4.

⁶⁰ See, e.g., Lichtblau and Risen, *supra* note 1, at A1; Bergman et al., *supra* note 2, at A1; CBS NEWS, *supra* note 2; American Civil Liberties Union, *supra* note 4.

⁶¹ 18 U.S.C. § 2709(a) (2006).

⁶² § 2709(b).

provision.⁶³ Pursuant to a certification, the FBI has the power to demand “the name, address, length of service, and local and long distance toll billing records of a person or entity.”⁶⁴

The certification required under § 2709 must state that the records sought “are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.”⁶⁵ This law was amended by the USA PATRIOT Act of 2001 to remove a requirement that the FBI limit its requests to information on “foreign powers” as defined by the FISA.⁶⁶ Before it was amended, 18 U.S.C. § 2709(b)(1)(B) required certification that “there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801).”⁶⁷ As it now stands, the statute allows the FBI to demand disclosure of records pertaining to purely domestic communications between American citizens.⁶⁸

An FBI certification may prohibit the telecommunications provider from whom records are requested from disclosing that a request for records has been made.⁶⁹ Under 18 U.S.C. § 2709, the individual making the certification need only state that “there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person” if the fact that a request for records was made is revealed to the public.⁷⁰ If such a statement accompanies the certification requesting disclosure of records:

⁶³ See Federal Bureau of Investigation, *Your Local FBI Office*, <http://www.fbi.gov/contact/fo/fo.htm> (last visited Apr. 16, 2008).

⁶⁴ 18 U.S.C. § 2709(b).

⁶⁵ *Id.*

⁶⁶ See Pub. L. No. 107-56, § 505(a)(2).

⁶⁷ 18 U.S.C. § 2709(b)(1)(B) (1994) (amended 2001).

⁶⁸ § 2709(b)(1).

⁶⁹ § 2709(c)(1).

⁷⁰ *Id.*

[N]o wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.⁷¹

Therefore, telephone companies that receive an FBI request for customer records may be statutorily prohibited from disclosing the fact of that request. Companies from which the FBI demands phone records may reveal the demand to their attorneys in order to seek legal advice, but must inform counsel of the non-disclosure requirement.⁷² Attorneys who are informed of a request are, in turn, prohibited from disclosing the fact of that request to any outside party.⁷³ The non-disclosure provision is not subject to any time limitation.⁷⁴

As with disclosures of customer records made pursuant to a warrant, court order, or administrative subpoena, telephone companies that disclose customer records pursuant to an FBI certification are granted blanket immunity from both criminal and civil liability.⁷⁵ 18 U.S.C. § 2703(e) specifies that “[n]o cause of action shall lie in any court against any provider of wire or electronic communication service . . . for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.”⁷⁶ This provision is also contained in Chapter 121 of the United States Code, the same Chapter that includes 18 U.S.C. § 2709.

⁷¹ *Id.*

⁷² § 2709(c)(3).

⁷³ *Id.* Without this statutory provision, attorney-client privilege would prohibit attorneys from revealing information conveyed by telecommunications clients seeking legal advice. The statute’s main effect is to prohibit attorneys from publicizing the fact that their telecommunications clients have received an information request from the federal government even in cases where the client explicitly waives privilege by giving the attorney permission to publicize the fact that an information request has been made.

⁷⁴ *Id.*

⁷⁵ 18 U.S.C. § 2703(e) (2006).

⁷⁶ *Id.*

Furthermore, since 18 U.S.C. § 2709 outlines the only procedure in that Chapter in which a “certification” (as opposed to a warrant, court order, or administrative subpoena) may be used by a government agency to request telephone records, the immunity granted by 18 U.S.C. § 2703(e) must apply to FBI certifications.⁷⁷ Any other interpretation of the statute would make the word “certification” unnecessary.⁷⁸ Therefore, telecommunications providers are immune from all potential civil and criminal liability arising out of their disclosure of customer records pursuant to an FBI certification.

Once customer records are disclosed to the FBI, it may distribute the records to any other government agency.⁷⁹ The FBI is allowed to disseminate records disclosed pursuant to a certification as long as the distribution is conducted in accordance with guidelines approved by the Attorney General and “such information is clearly relevant to the authorized responsibilities of such agency.”⁸⁰ Under this standard, no check outside of the executive branch limits the distribution of confidential telephone records between the FBI and other government agencies. As long as the agency receiving records from the FBI is involved in combating terrorism, the records collected by the FBI pursuant to counterterrorism investigations may be disclosed.⁸¹

Given reports that recent government requests for disclosure of telephone company records were made without a warrant or court order,⁸² it is likely that the requests were made pursuant to either an administrative subpoena or an FBI certification. There are three factors that make it highly likely that the process of FBI certifications has been used in at least some data mining cases in order to gain access to telephone customer records: (1) the ease with which an FBI certification can be made; (2) the fact that the FBI can disseminate

⁷⁷ *See id.*

⁷⁸ *See, e.g., Regions Hosp. v. Shalala*, 522 U.S. 448, 467 (1998) (“We are not at liberty to construe any statute so as to deny effect to any part of its language. It is a cardinal rule of statutory construction that significance and effect shall, if possible, be accorded to every word.”) (quoting *Washington Mkt. Co. v. Hoffman*, 101 U.S. 112, 115–16 (1879)) (internal quotations omitted).

⁷⁹ *See* 18 U.S.C. § 2709(d) (1994).

⁸⁰ *Id.*

⁸¹ *See id.*

⁸² *See, e.g., Lichtblau and Risen, supra* note 1, at A1; *Bergman et al., supra* note 2, at A1; *CBS NEWS, supra* note 2; *American Civil Liberties Union, supra* note 4.

records received pursuant to a certification to other agencies engaged in counterterrorism operation; and (3) the FBI's ability to unilaterally prohibit telephone companies from revealing the existence of a records request. In light of the classified nature of the data mining program, however, it is impossible to know the exact statutory basis underlying the requests.

C. SUMMARY OF STATUTES REQUIRING DISCLOSURE

Companies must disclose customer records requested by a government entity (1) pursuant to a warrant,⁸³ (2) when served with a court order,⁸⁴ (3) when presented with a formal written request for records relevant to a law enforcement investigation concerning telemarketing fraud,⁸⁵ (4) when served with an administrative subpoena,⁸⁶ or (5) pursuant to an FBI certification that the records are relevant to an ongoing counterterrorism investigation.⁸⁷ Telephone companies must retain customer records that have been requested by a government entity for ninety days pending the issuance of a warrant, court order, administrative subpoena, or FBI certification.⁸⁸ The government may renew the ninety-day retention period indefinitely.⁸⁹ Phone companies that disclose customer records pursuant to a warrant, court order, administrative subpoena, or FBI certification are granted immunity from both civil and criminal liability.^{90*}

⁸³ 18 U.S.C. § 2703(c)(1)(A) (2006).

⁸⁴ § 2703(c)(1)(B).

⁸⁵ § 2703(c)(1)(D).

⁸⁶ § 2703(c)(2).

⁸⁷ 18 U.S.C. § 2709 (1994).

⁸⁸ 18 U.S.C. § 2703(f)(1) (2006).

⁸⁹ § 2703(f)(2).

⁹⁰ 18 U.S.C. § 2703(e) (2006).

* At the time of writing, there were over 40 civil suits pending against major telecommunications providers based on the claim that those providers violated customer privacy protections by disclosing records and allowing government surveillance of customer conversations. In February, 2008, the United States Senate passed a bill that would have granted blanket retroactive immunity to telecommunications carriers who disclosed records or allowed surveillance of customer conversations. However, the House of Representatives failed to pass a similar version of the bill, thereby preventing it from

IV. TELEPHONE COMPANY INCENTIVES AND THE DEMISE OF CUSTOMER PRIVACY

By utilizing a little-known statutory scheme to compel disclosure of otherwise confidential records, the government's data mining program creates perverse incentives for telephone companies to compromise the privacy expectations of their customers. In light of the general prohibition on disclosure of customer records, the statutory scheme contained in 18 U.S.C. §§ 2703 and 2709 is troubling.⁹¹ The specific nature of the amendments to 18 U.S.C. § 2709 contained in the USA PATRIOT Act was not widely publicized, and members of the general public may still be under the impression that their telephone records cannot be legally revealed to government agencies.⁹² Since telephone companies are insulated from all civil and criminal liability arising out of disclosures, but are not insulated from government retaliation for failure to comply, they will find it in their self-interest to cooperate with government requests rather than protect their customers' privacy.⁹³ The incentives for cooperation have been borne out by the fact that only one major telephone company refused to comply with government requests for records.⁹⁴ Other companies complied with the program, while simultaneously stating that they highly valued the privacy of their customers and would do "everything . . . 'within the law'" to protect it.⁹⁵

becoming law. The issue of retroactive immunity for telecommunications carriers was reportedly one of the main points of contention that led to the bill's demise. It is unclear whether Congress will revisit the issue of retroactive immunity in later legislation. Furthermore, the question of how courts will deal with the statutory immunity granted under existing law has not yet been resolved. *See Senate OKs Immunity for Telecoms in Intelligence Bill*, CNN NEWS, Feb. 12, 2008, <http://www.cnn.com/2008/POLITICS/02/12/fisa.senate/index.html>; *House Likely to Let Surveillance Law Lapse*, CNN NEWS, Feb. 13, 2008, <http://www.cnn.com/2008/POLITICS/02/13/fisa.bush/index.html>.

⁹¹ *See* 47 U.S.C. § 222 (1999); 18 U.S.C. § 2702 (2006).

⁹² *See* CBS NEWS, *supra* note 2 (quoting various Congressional representatives regarding the "privacy crisis" created by the data mining program).

⁹³ *See* 18 U.S.C. § 2703(e) (2006).

⁹⁴ CBS NEWS, *supra* note 2 (noting that "the only telecom giant to refuse the government's request was Qwest, which serves 14 million customers in the West and Northwest").

⁹⁵ *Id.*; *see also* Lichtblau and Risen, *supra* note 1, at A1; Bergman et al., *supra* note 2, at A1.

The overwhelming incentive for telephone companies to cooperate with government requests for records is especially troubling when examined in light of the fact that telephone companies may be forbidden by the terms of an administrative subpoena or FBI certification from revealing that such a request has been made.⁹⁶ Since government agencies need not inform telephone customers that their records have been requested,⁹⁷ it is highly unlikely that an individual whose records were disclosed would ever learn of the disclosure. The virtual impossibility of any given individual ascertaining whether his or her records were disclosed to the government creates a collective action problem due to the fact that it will be difficult to mobilize public opinion to advocate for the privacy of records when the particular victims of the program cannot be identified. The government can, in essence, characterize the program as being limited to “terrorists” or some form of sociological “other” and thereby claim that “ordinary Americans” are unaffected. When attempting to justify the data mining program shortly after media reports about it emerged, the government did just that.⁹⁸

V. DATA MINING AS AN INEFFICIENT USE OF GOVERNMENT RESOURCES

More troubling than the data mining program’s implications for privacy rights is the fact that it is an extremely inefficient method of investigating possible terrorist activity. Media reports cite multiple sources within the counterterrorism community who complain that the data mining program wastes the limited time and resources of government investigators by creating millions of false positive suspect identifications that then must be eliminated through more traditional investigatory methods.⁹⁹ The New York Times reported that the NSA referred such a large number of suspects to the FBI for investigation that “hundreds of agents” had to be diverted in an effort “to check out thousands of tips a month.”¹⁰⁰ According to FBI agents, the large

⁹⁶ See 18 U.S.C. § 2709(c)(3) (2006); 18 U.S.C. § 2703 (2006).

⁹⁷ See 18 U.S.C. § 2703(c)(3) (2006).

⁹⁸ See, e.g., Lichtblau and Risen, *supra* note 1, at A1; Bergman et al., *supra* note 2, at A1; CBS NEWS, *supra* note 2; American Civil Liberties Union, *supra* note 4.

⁹⁹ See, e.g., Bergman et al., *supra* note 2, at A1; CBS NEWS, *supra* note 2.

¹⁰⁰ Bergman et al., *supra* note 2, at A1.

amount of tips received from the data mining program led to few potential terrorists who had not been discovered by using more traditional investigative tactics, and “diverted agents from counterterrorism work they viewed as more productive.”¹⁰¹ It is impossible, in light of the dual constraints of budgetary resources and limited personnel, for the government to investigate every potential lead regardless of the degree of likelihood that it may result in the detection of a terrorist plot. Therefore, government agents and resources should be allocated to the most promising leads—the ones most likely to preempt an attack—in order to save the maximum amount of American lives.

VI. CONCLUSION: TRADITIONAL TECHNIQUES AND COUNTERTERRORISM

Traditional investigative tools that rely on particularized suspicion, as opposed to a wide dragnet of communications records and other data, present a more effective and more efficient means of investigating potential terrorists. Under a more traditional investigative model, raw data is narrowed by the requirement that investigators meet some threshold of suspicion before gaining access to confidential information concerning a suspect.¹⁰² In the case of counterterrorism, the requirement that some threshold of suspicion be established before an individual is considered a suspect would narrow the focus of government agents and assure that limited government resources are used to investigate those individuals who are most likely to pose a threat. In short, it would force the government to conserve resources by prioritizing their suspects.

Such prioritization is desirable for a number of reasons. As mentioned above, the resources devoted to combating terrorism are, while considerable, necessarily finite. If hundreds of government agents find their time monopolized by the requirement that they sift through mountains of raw data and eliminate thousands of suspects with no apparent ties to international terrorism other than anomalous patterns in their telephone records, those agents are not spending their time investigating individuals who have been identified as

¹⁰¹ *Id.*

¹⁰² The probable cause requirement of U.S. CONST. amend. IV, and reasonable suspicion requirement of *Terry v. Ohio*, 392 U.S. 1 (1968), serve as examples of the different thresholds of suspicion required for varying levels of intrusion by government agents.

potential terrorists by informants or other traditional law enforcement methods.

A second benefit of prioritizing terrorism suspects by utilizing traditional law enforcement methods is presented by the ongoing nature and potential long-term benefits of those investigatory techniques. Data mining generates information on the telephone communication patterns of a single individual. That information is only useful in investigating the individual to whom it applies. In contrast, traditional law enforcement methods such as cultivating informants within terrorist organizations, mapping the movement of suspects through first-hand surveillance, and interrogating suspects in order to “flip” them and force them to turn over their colleagues, have collateral benefits beyond the original investigation. Informants can be utilized in the future. Once an organization’s safe houses and preferred methods of travel are discovered, those areas and transportation routes can be monitored for future activity. When an individual being interrogated informs police as to the identity of his co-conspirators, those identities can be used to generate future investigations and arrests, or to create future informants by pressuring individuals with the threat of legal action and punishment.

Finally, a prioritization of terrorism suspects by requiring some threshold of suspicion before an investigation of an individual proceeds has the added benefit of assuring the privacy of those whom authorities have no reason to believe are involved in terrorism. That benefit, which is traditionally protected by the requirement that law enforcement show “probable cause” before searching or seizing an individual, is compromised by data mining and other programs which depend on confidential bits of information innocent in and of themselves, that are compiled and used to detect suspicious patterns of behavior.

